REMARKS

Claims 1-30 were pending and under consideration.

In the Office Action of October 6, 2005, claim 1-30 were rejected. Claim 1, 8, 9, 14-16 and 30 were rejected as obvious in view of Dulude et al. (USP 6310966) and Bianco et al (USP 6,256,737). Claims 2-6, 10, 11, 18-22 and 26-27 were rejected as obvious in view of Dulude et al., Bianco et al, and Arnes ("Public Key Certification Revocation Schemes," Master Thesis, Queen's Univeristy, February, 2000). Claims 7, 13 and 29 were rejected as obvious in view of Dulude et al., Bianco et al. and Diffie ("Authentication and Authenticated Key Exchanges," Designs, Codes and Cryptography, Kluwer Academic Pulishers, 1992). Claims 12 and 28 were rejected as obvious in view of Dulude et al., Bianco et al. and Yu et al. (USP 5930804).

In response, without conceding to the position taken by the examiner in the Office Action, and without waiving any right to challenge the arguments, including proving an invention date prior to that of Dulude et al., the independent claims 1, 17 and 30 have been amended to recite that: "the public key used to encrypt or decrypt the template stored in the person identification certificate being a different public key depending upon the entity which executes authentication of a person"

Regarding the rejections of the claims under 35 USC 103, it is submitted that the amendments to the independent claims overcomes the rejections, regardless of whatever arguments applicants may have or whatever proof of prior invention they may have.

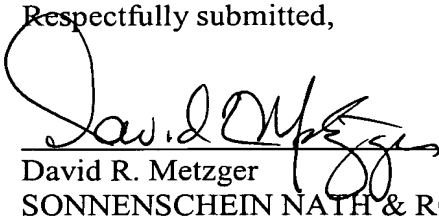
In that regard, the claims require that a person identification authority acquires a template and data from a person to be identified and then creates an identification certificate in which is stored an encrypted template with the person identifying data. The template is encrypted with a public key. Additionally the claims require that when a user is to be authenticated, the template is decrypted by a person authentication entity and compared with sampling information of the user. Finally, the public key used to encrypt or decrypt the template stored in the person identification certificate is a different public key depending upon the entity which executes authentication of a person.

The result is a system that provides for a single registration step yet allows for distributed authentication locations and environments as the various entities which perform an authentication step can utilize a different public key. Further, the authentication information can be stored and transmitted in a reliably secure manner.

It is submitted that none of the references, nor any combination of them, fairly discloses or suggests these features in a user authentication system.

In view of the foregoing, it is submitted that claims 1-30 are allowable and that the application is in condition for allowance. Notice to that effect is requested.

Respectfully submitted,



(Reg. No. 32,919)

David R. Metzger
SONNENSCHEIN NATH & ROSENTHAL LLP
P. O. Box 061080
Wacker Drive Station - Sears Tower
Chicago, Illinois 60606-1080
Telephone (312) 876 8000
Customer No. 26263